

Fuites de données, mode d'emploi

Pourquoi des fuites de données se produisent-elles et comment s'en prémunir ?

Fuites de données, mode d'emploi

Pourquoi des fuites de données se produisent-elles et comment s'en prémunir ?

Sommaire

Introduction	1
Pourquoi les fuites de données se produisent-elles ?	2
Employés bien intentionnés	2
Attaques ciblées	3
L'employé malveillant	6
Quelles conclusions tirer de tout cela ?	6
Comment mettre fin aux fuites de données ?	7
Comment démarrer ?	10
Pourquoi choisir Symantec ?	10
Annexe	12

Introduction

Pour les entreprises qui détiennent des informations stratégiques (données sur les clients, propriété intellectuelle, secrets professionnels, informations propriétaires, etc.), le risque de fuites est plus élevé qu'il ne l'a jamais été. En fait, le nombre d'enregistrements électroniques détournés en 2008 est même supérieur à celui des quatre années précédentes réunies.¹

Cette recrudescence des fuites de données n'est en aucune manière surprenante. Dans un monde où les données sont omniprésentes, les entreprises ont plus de difficultés que jamais à protéger les informations confidentielles. La complexité et l'hétérogénéité des environnements informatiques rendent la protection des données et les réponses aux menaces particulièrement compliquées. Les entreprises d'aujourd'hui dépendent de leurs équipes de sécurité pour faire en sorte que la collaboration et le partage des données par des employés toujours plus mobiles continuent à s'effectuer sans risque.

Si le flux continu des fuites de données est bien documenté, les raisons de ces fuites et les actions possibles pour les empêcher sont beaucoup moins bien comprises. Le présent document examine les trois sources de fuites de données les plus courantes (employés internes bien intentionnés, employés malveillants et attaques ciblées extérieures à l'entreprise) et pour chacune de ces sources, explique comment l'individu concerné accède au réseau, localise puis expose les informations sensibles. Ce document propose également un large survol des actions possibles pour mettre fin à ces fuites ainsi que des conseils spécifiques sur les moyens de les prévenir. La section intitulée *Quelles conclusions tirer de tout cela ?* offre un point de vue unique sur les fuites de données qui s'appuie sur l'avis des experts du marché en matière de sécurité, sur les données d'un vaste réseau d'informations international et sur la longue expérience de Symantec dans l'assistance des clients et la protection des données sensibles.

1-Equipe Verizon chargée de la gestion des risques économiques, rapport d'enquête 2009 sur les fuites de données

Pourquoi les fuites de données se produisent-elles ?

Pour prévenir une fuite de données, il est essentiel de comprendre pourquoi elle se produit. Les recherches de sociétés tierces sur les causes des fuites de données, collectées par l'Equipe Verizon chargée de la gestion des risques économiques² et la Open Security Foundation³, mettent en lumière trois types de causes : employés internes bien intentionnés, employés malveillants et attaques ciblées. Dans bon nombre de cas, les fuites sont causées par une combinaison de ces facteurs. Par exemple, les attaques ciblées sont souvent rendues possibles par des employés bien intentionnés qui oublient d'appliquer les politiques de sécurité, ouvrant ainsi la porte aux éventuelles fuites.⁴

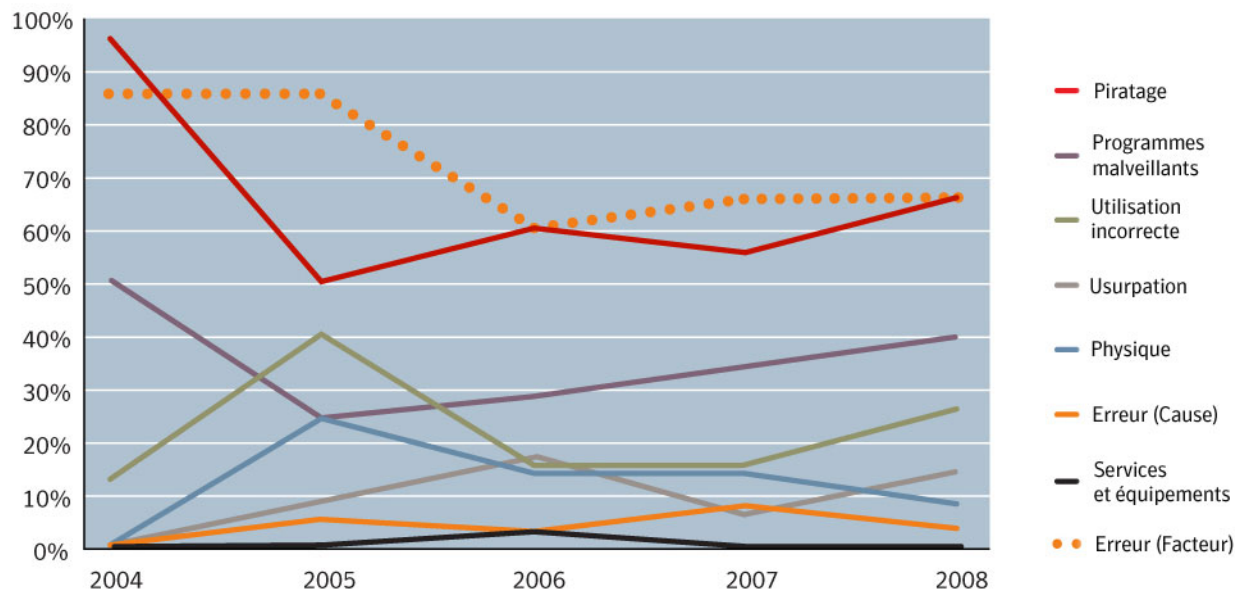


Figure 1. Tendances dans les causes de fuites de données, 2004–2008

Employés bien intentionnés

Les employés qui oublient d'appliquer les consignes de sécurité aux données de leur entreprise continuent de représenter la cause majeure de fuites. Selon le rapport Verizon, 67% des fuites de l'année 2008 ont été facilitées par des "erreurs significatives" émanant d'employés bien intentionnés.⁵ Dans une enquête de 2008 auprès de 43 entreprises ayant eu à subir des fuites de données, l'Institut Ponemon constatait que dans 88 % des cas, des négligences du personnel étaient à l'origine de ces fuites.⁶ Une analyse des fuites de données provoquées par des employés bien intentionnés fait ressortir cinq principaux types de fuites :

- **Données exposées sur les serveurs et les ordinateurs de bureau.** La prolifération quotidienne d'informations sensibles sur les serveurs, ordinateurs de bureau et ordinateurs portables non protégés est la conséquence naturelle d'employés hautement productifs. Le type de fuite le plus courant semble être celui qui se produit quand des employés, bien intentionnés mais non informés des consignes de sécurité de l'entreprise, enregistrent, envoient ou copient des informations sensibles non chiffrées. Dans l'éventualité où un pirate

2-Ibid.

3-<http://datalossdb.org/>

4-Verizon Business Risk Team (voir plus haut)

5-Ibid.

6-Institut Ponemon, étude annuelle 2008 : coût d'une fuite de données, février 2009

parviendrait à accéder à votre réseau, vos fichiers confidentiels stockés ou utilisés en l'absence de tout chiffrement seraient vulnérables et faciles à détourner. En raison de la croissance exponentielle des données, les entreprises d'aujourd'hui ne disposent d'aucun moyen pour connaître exactement la quantité d'informations sensibles présente sur leurs systèmes. L'ignorance de l'entreprise quant à l'emplacement des données stockées sur ses systèmes a représenté 38 % des causes de fuites en 2008 (et les enregistrements concernés représentaient 67% des enregistrements détournés).⁷

- **Ordinateurs perdus ou volés.** L'enquête 2008 de l'Institut Ponemon révèle que les ordinateurs perdus ont été la cause première des fuites de données pour 35 % des entreprises interrogées.⁸ Dans les grandes entreprises, c'est chaque semaine que des ordinateurs portables disparaissent. Même quand ces disparitions ne s'accompagnent pas de vols d'identité, les lois sur la déclaration des fuites de données font de ces pertes d'ordinateur une source d'embarras et de dépenses considérables.
- **Messagerie, messagerie Internet et périphériques amovibles.** Les évaluations de risques réalisées par Symantec pour ses clients potentiels montre qu'en moyenne, un message électronique sur 400 contient des données confidentielles non chiffrées.⁹ Les transmissions réseau de ce type représentent un risque de perte de données important. Dans le scénario classique, un employé transmet des données confidentielles à un compte de messagerie personnel ou copie ces dernières sur une clé USB, un CD ou un DVD afin de pouvoir travailler le week-end. Dans ce scénario, les données sont doublement exposées : durant la transmission elle-même et sur l'ordinateur familial ou le périphérique amovible éventuellement non protégé.
- **Pertes de données imputables à des tiers.** Les relations professionnelles avec les partenaires et les fournisseurs impliquent souvent l'échange d'informations confidentielles telles que celles relatives à un plan de retraite, au traitement externalisé des règlements, à la gestion de la chaîne logistique, et autres types de données opérationnelles. Le risque de fuites de données augmente encore lorsque le partage des données est trop étendu ou que les partenaires s'abstiennent de mettre en application les politiques de sécurité nécessaires. Le rapport Verizon signale l'implication de partenaires professionnels dans 32 % des fuites de données.¹⁰
- **Les processus de gestion automatisent la diffusion des données sensibles.** L'une des causes de prolifération des données sensibles est l'existence de processus de gestion inappropriés ou obsolètes qui distribuent automatiquement ces données à des personnes non autorisées ou à des systèmes non protégés où elles peuvent être aisément détournées par des pirates ou volées par des employés malveillants. Les évaluations des risques sur site réalisées par Symantec montrent que dans presque 50 % des cas, ce sont des processus de gestion obsolètes ou non autorisés qui sont responsables de l'exposition régulière des données sensibles.

Attaques ciblées

Dans le monde interconnecté d'aujourd'hui, où les données sont omniprésentes et où "le périmètre" peut se trouver n'importe où, la protection des informations face à des techniques de piratage hautement sophistiquées relève véritablement du défi. Portées par une vague de cybercriminalité organisée sans précédent, les attaques ciblées visent de plus en plus le détournement des informations à des fins de vol d'identité. Plus de 90 % des enregistrements volés en 2008 l'ont été par des groupes identifiés par les autorités compétentes comme relevant du crime organisé.¹¹ Ces attaques

7-Equipe Verizon chargée de la gestion des risques économiques (voir plus haut)

8-Institut Ponemon (voir plus haut)

9-Evaluation des risques par Symantec dans le cadre de la prévention des pertes de données

10-Verizon Business Risk Team (voir plus haut)

11-Ibid

sont souvent automatisées au moyen d'un code malveillant capable de s'infiltrer dans l'entreprise à son insu, puis d'exporter les données vers des sites pirates distants. En 2008, Symantec a créé plus d'1,6 million de signatures de codes malveillants (un chiffre supérieur à celui des 17 années précédentes combinées) et bloqué en moyenne 245 millions d'attaques de code malveillants par mois d'un bout à l'autre du globe.¹²

Évalués en fonction du nombre d'enregistrements compromis, les accès non autorisés faisant appel à des noms et mots de passe d'utilisateur par défaut ou partagés, à des listes de contrôle d'accès (ACL) insuffisamment restreintes et à des injections de SQL ont été de loin les types d'attaques les plus courants en 2008.¹³ Par ailleurs, 90 % des enregistrements perdus étaient imputables au déploiement de programmes malveillants.¹⁴ La première phase de l'attaque (l'incursion initiale) se déroule généralement de l'une de ces quatre manières :

- **Vulnérabilités des systèmes.** Bien souvent, les ordinateurs portables, les ordinateurs de bureau et les serveurs ne disposent pas des tous derniers correctifs de sécurité, ce qui crée une faille dans le dispositif de sécurité global. Une configuration incorrecte des ordinateurs ou de la sécurité peut également engendrer des failles ou des vulnérabilités dans les systèmes. Les cybercriminels recherchent ces faiblesses et les exploitent pour obtenir l'accès au réseau et aux informations confidentielles de l'entreprise.
- **Noms d'utilisateur et mots de passe inappropriés.** Les mots de passe des systèmes couplés à Internet, tels que les serveurs de messagerie, les serveurs Web ou les serveurs FTP, sont souvent laissés avec les valeurs par défaut d'usine, lesquelles peuvent être facilement obtenues par les pirates. Les listes de contrôle d'accès insuffisamment restreintes ou obsolètes peuvent constituer des opportunités pour les pirates ou les employés malveillants.
- **Injection SQL.** En analysant la syntaxe de l'URL des sites Web ciblés, les pirates parviennent à injecter des instructions déclenchant le téléchargement de logiciels espions qui leur donnent accès aux serveurs cibles.
- **Attaques ciblées de programmes malveillants.** Les pirates ont recours au spam, aux messages électroniques et aux messages instantanés, souvent maquillés en messages de personnes connues, pour diriger les utilisateurs vers des sites Web compromis par des programmes malveillants. Dès qu'un utilisateur visite un site compromis, le programme malveillant peut être téléchargé avec l'accord de cet utilisateur ou à son insu. Des appâts tels que les *logiciels gratuits* incitent cet utilisateur à télécharger un logiciel espion qui permet de surveiller l'activité de ce dernier sur le Web et de capturer les informations qu'il utilise fréquemment, comme les données de connexion et les mots de passe d'une entreprise. Les outils d'accès à distance (RAT) sont des exemples de logiciels espions téléchargés automatiquement vers le PC d'un utilisateur, à l'insu de ce dernier. Ils permettent au pirate de prendre le contrôle de cette machine et d'accéder aux informations d'une entreprise depuis un site distant.

Pour protéger les données, la plupart des équipes de sécurité se focalisent presque exclusivement sur l'arrêt des incursions. Cependant, l'incursion n'est que la première phase d'une fuite de données par attaque ciblée. Pour assurer une protection complète, il est indispensable de traiter les quatre phases.

Les quatre phases d'une attaque ciblée : incursion, découverte, capture, exfiltration.

12-Rapport Symantec Internet Security Threat Report, Volume XIV
13-Verizon Business Risk Team (voir plus haut)
14-Ibid

- **Phase 1 : Incursion.** Les pirates pénètrent dans le réseau d'une entreprise en exploitant les vulnérabilités du système à l'aide de diverses techniques (violation de mot de passe par défaut, injection SQL ou attaques ciblées de logiciels malveillants).
- **Phase 2 : Découverte.** Les pirates établissent une cartographie des systèmes de l'entreprise et lancent une recherche automatique des données confidentielles.
- **Phase 3 : Capture.** Le pirate accède immédiatement aux données que des employés bien intentionnés ont stockées sur des systèmes non protégés. Par ailleurs, des composants appelés root kits sont subrepticement installés sur les systèmes ciblés et points d'accès réseau en vue de capturer les données confidentielles au fur et à mesure qu'elles circulent dans l'entreprise.
- **Phase 4 : Exfiltration.** Les données confidentielles sont envoyées à l'équipe du pirate au grand jour (par messagerie Internet, par exemple) dans des paquets chiffrés ou dans des fichiers zip protégés par mot de passe.

La bonne nouvelle est qu'une attaque ciblée visant des données confidentielles peut être bloquée durant n'importe laquelle de ces quatre phases. Les professionnels de la sécurité qui se focalisent exclusivement sur la phase d'incursion font un pari de type "tout ou rien" qu'ils finiront par perdre tôt ou tard, compte tenu de l'environnement informatique totalement ouvert d'aujourd'hui. En s'efforçant de prévenir la découverte, la capture et l'exfiltration des données, les entreprises peuvent considérablement renforcer leurs défenses contre les attaques ciblées.

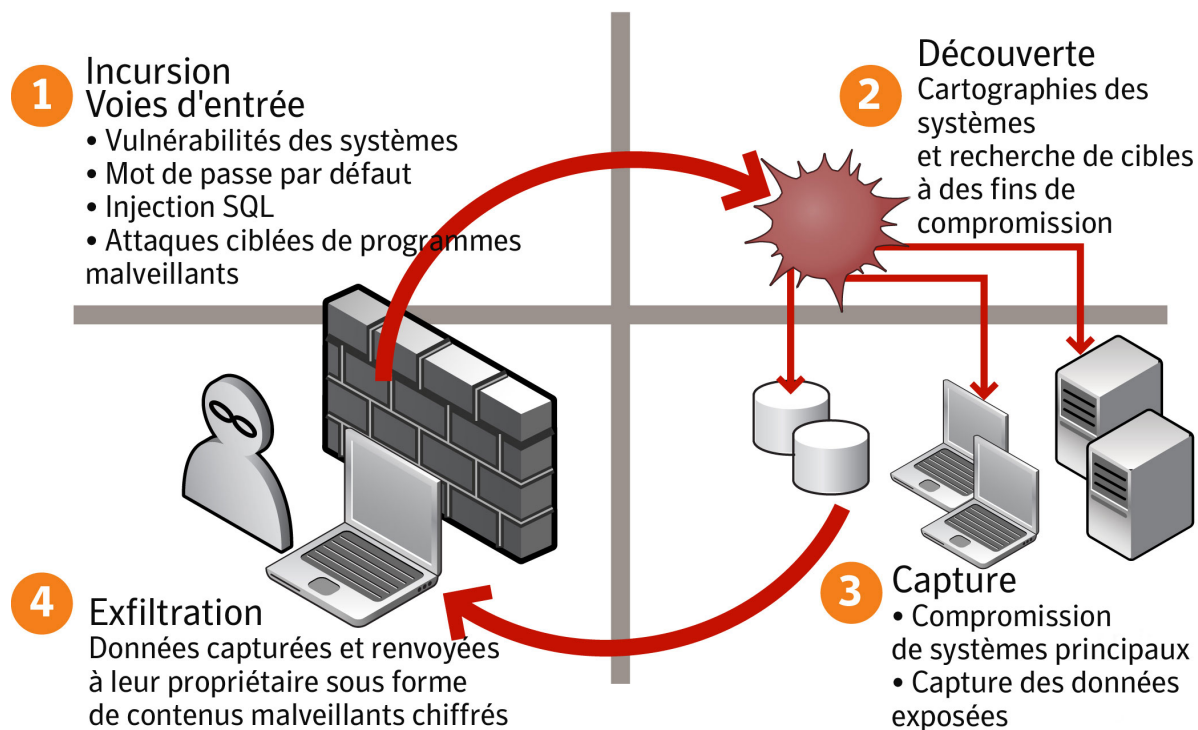


Figure 2. Quatre phases d'attaques ciblées

L'employé malveillant

Les employés malveillants sont à l'origine d'un segment croissant de fuites de données et d'un segment proportionnellement plus grand encore de coûts associés à ces fuites. L'étude Ponemon a montré que le coût des fuites de données imputables à des négligences est de 199 dollars par enregistrement tandis que celui des fuites provoquées par des actes de malveillance s'élève à 225 dollars par enregistrement.¹⁵ Les fuites causées par des employés ayant l'intention de voler des informations peuvent être classées en quatre groupes :

- **Le crime en col blanc.** L'employé qui dérobe sciemment des données dans le cadre d'un réseau de vol d'identité est devenu une figure hautement familière dans les annales du crime en col blanc. Les opérations de ce type sont perpétrées par des employés de l'entreprise qui abusent de leurs privilèges d'accès aux informations pour en tirer un gain personnel.
- **Employés licenciés.** En ces temps de crise économique, avec leur lot de licenciements quotidiens, les fuites de données imputables à des anciens salariés mécontents sont devenues chose courante. Bien souvent, l'employé est informé de son licenciement avant que son accès à des services tels qu'Active Directory ou Exchange ait été désactivé, ce qui offre à ce dernier l'opportunité d'accéder à des données confidentielles, puis de les transmettre par courrier électronique à un compte privé ou de les copier sur un support amovible. Une étude récente des effets des licenciements sur la sécurité des données a révélé que 59 % des anciens salariés emportaient avec eux des données de l'entreprise, notamment, des listes de clients et des dossiers d'employés.¹⁶
- **Employés qui cherchent à faire carrière en exploitant les données de l'entreprise.** Il est courant que des employés transfèrent sur leur ordinateur familial des données de leur entreprise en vue de se constituer une bibliothèque d'échantillons de travail pouvant leur servir par la suite pour des opportunités de carrière. Bien que de tels actes ne puissent être à proprement parler considérés comme malveillants en termes de vol d'identité, les conséquences peuvent être tout aussi désastreuses. Si, en cas de piratage de l'ordinateur familial, les données en question sont dérobées, le dommage subi par l'entreprise et ses clients sera le même.
- **Espionnage industriel.** Le dernier type d'employé malveillant est représenté par le salarié malheureux ou peu performant qui, décidé à démissionner, envoie des exemples de son travail à une société concurrente dans le cadre du processus de candidature et d'évaluation d'embauche. Les informations détaillées sur les produits, les plans marketing, les listes de clients et les données financières sont exposées à ce type d'utilisation.

Quelles conclusions tirer de tout cela ?

Au rythme quasi-quotidien où les fuites de données font la une des journaux, on peut être tenté de les considérer comme des sous-produits inévitables de notre monde interconnecté, un coût parmi tant d'autres de notre activité avec lequel nous devons tout simplement apprendre à vivre. Toutefois, il suffit de regarder les faits d'un peu plus près pour voir que ce n'est pas nécessairement le cas. Symantec apporte son expertise en matière de sécurité, un réseau d'informations international et une expérience pratique auprès des clients, et une telle combinaison d'avantages ouvre des perspectives un peu plus optimistes. Vue sous cet angle, la prise de contrôle du problème des fuites de données passe par la reconnaissance de trois vérités essentielles.

¹⁵-Institut Ponemon (voir plus haut)

¹⁶-Institut Ponemon, "Risque de perte de données en période de réduction des effectifs : les employés s'en vont... avec les données de l'entreprise", 2008

Premièrement, il est possible de prévenir ces fuites. Dans chacun des scénarios de fuite commentés plus haut, il existait des étapes d'intervention pendant lesquelles des contre-mesures auraient pu empêcher la fuite (et dans certains cas y sont parvenues). Contrairement à l'impression laissée par la couverture sensationnaliste de certains médias, il y a de bonnes raisons d'être optimiste.

Deuxièmement, les seules stratégies qui ont une chance de succès sont celles qui sont fondées sur les risques et qui sont sensibles au contenu. La prévention des fuites de données est avant tout une question de réduction des risques. Or, pour réduire les risques, il est nécessaire que vous connaissiez l'emplacement de stockage des données, leur destination et la façon dont elles sont utilisées. Ce n'est qu'à cette condition que vous pourrez identifier clairement les pratiques qui posent problème, hiérarchiser les données et les groupes afin de prendre des mesures de correction par phase et commencer à réduire le flux des informations qui sortent de votre entreprise.

Troisièmement, la prévention des fuites passe par la mise en oeuvre de solutions multiples qui opèrent ensemble pour résoudre le problème. Il ne s'agit donc pas d'une simple défense en profondeur, loin de là. Autrement dit, il faut que les solutions que vous déployez (qu'il s'agisse de surveiller les informations, de protéger les terminaux, de vérifier les contrôles techniques et procéduraux, de consolider les systèmes de base ou de mettre en oeuvre des alertes en temps réel) soient intégrées de manière à constituer une vue centralisée de la sécurité des informations qui vous permette d'établir des corrélations et de découvrir rapidement et de façon décisive l'origine des problèmes.

Comment mettre fin aux fuites de données ?

Pour surveiller leurs systèmes et mettre les informations à l'abri des menaces internes et externes à tous les niveaux de l'infrastructure informatique, les entreprises doivent sélectionner des solutions qui reposent sur un modèle de sécurité opérationnel fondé sur les risques et sensible au contenu, immédiatement réactif aux menaces et piloté par workflow afin d'automatiser les processus de sécurité des données. Voici, divisées en six étapes, les mesures que toute entreprise peut prendre pour réduire sensiblement les risques de fuites au moyen de solutions éprouvées :

Etape 1. Mettre fin aux incursions par attaque ciblée. Les quatre principaux moyens d'incursion employés par les pirates pour accéder au réseau d'une entreprise sont l'exploitation des vulnérabilités des systèmes, la violation des mots de passe par défaut, les injections SQL et les attaques de programmes malveillants ciblées. Pour prévenir ces incursions, il est nécessaire de fermer chacune de ces voies d'accès aux informations de l'entreprise. Pour mettre fin aux attaques, les entreprises doivent combiner les solutions d'évaluation des contrôles automatisées et celles de protection des systèmes de base, de sécurité des terminaux, du Web et de la messagerie. Il convient en outre de gérer les terminaux de façon centralisée afin de garantir un déploiement cohérent des politiques de sécurité, des correctifs, des fonctions de chiffrement et de l'accès aux informations.

- Mettre en oeuvre des solutions de sécurité du Web, de la messagerie et des terminaux pour permettre la surveillance et le blocage des flux entrants de programmes malveillants.
- Mettre en place des systèmes de détection et de prévention des intrusions sur les serveurs pour sauvegarder l'intégrité des systèmes hôtes en cas d'attaque par injection SQL.
- Automatiser l'interrogation des administrateurs pour s'assurer que les mots de passe par défaut sont supprimés et les listes de contrôle d'accès à jour.

- Analyser automatiquement les contrôles techniques (y compris les contrôles de paramètres de mots de passe et de configuration de serveur) sur tous les serveurs du réseau et signaler toute violation des politiques.
- Centraliser le déploiement des politiques et l'administration des terminaux afin d'automatiser la gestion des correctifs et de garantir l'application des paramètres de chiffrement, de contrôle d'accès au réseau et de sécurité les plus récents.

Etape 2. Identifier les menaces en établissant des corrélations entre les alertes en temps réel à l'aide des informations de sécurité provenant du monde entier.

Pour faciliter l'identification des menaces d'attaques ciblées et la réponse à ces menaces, les systèmes de gestion des informations et des événements liés à la sécurité peuvent signaler toute activité réseau suspecte à des fins d'enquête. Ces alertes en temps réel sont encore plus précieuses quand les informations qu'elles procurent peuvent être mises en corrélation avec les informations disponibles sur des menaces réelles connues. La possibilité de bénéficier en temps réel des recherches et analyses actuellement réalisées sur la situation mondiale en matière de menaces confère aux équipes de sécurité un formidable avantage dans leur combat contre les menaces extérieures.

- Mettre à profit les services d'information sur la sécurité qui surveillent quotidiennement des millions de messages électroniques et de systèmes à travers le monde pour analyser les données relatives aux événements internes et se tenir informé de l'évolution des menaces.
- Combiner les informations sur la sécurité et les données des systèmes de gestion des événements pour suivre l'activité du réseau, collecter les données sur les incidents de tous les systèmes de sécurité et mettre en correspondance les journaux d'incidents et les données issues des services d'information de sécurité, afin d'identifier en temps réel les sites dangereux connus et autres menaces externes.

Etape 3. Protéger proactivement les informations. Dans le monde interconnecté d'aujourd'hui, défendre "le périmètre" n'est plus suffisant. Aujourd'hui, vous devez identifier précisément et protéger proactivement vos informations sensibles quel que soit le lieu où elles sont stockées, envoyées ou utilisées. En mettant en application des politiques de protection de données sur tous les serveurs, réseaux et terminaux de l'entreprise, vous pouvez réduire progressivement les risques de fuites de données. Les solutions de prévention des pertes de données peuvent faire de cette approche unifiée une réalité.

- Mettre en oeuvre une gestion de politiques sensible au contenu *définie une seule fois, mise en application partout* et offrant des processus de résolution des incidents, le reporting, la gestion des systèmes et la sécurité.
- Localiser les informations sensibles où qu'elles se trouvent (serveurs de fichiers, bases de données, référentiels de messagerie, sites Web, ordinateurs portables ou ordinateurs de bureau) et les protéger grâce à des fonctions de quarantaine et à la prise en charge du chiffrement fondé sur des politiques.
- Vérifier toutes les communications réseau sortantes telles que messages électronique, messages instantanés, FTP, P2P et TCP générique, et mettre en application des politiques de prévention des fuites d'informations confidentielles
- Empêcher proactivement les données confidentielles résidant sur des terminaux de quitter l'entreprise par le biais de l'impression, de la télécopie ou d'un support amovible.

Etape 4. Automatiser la sécurité par des contrôles de conformité des ressources informatiques. Pour prévenir les fuites de données, les entreprises doivent commencer par développer des politiques et les mettre en application sur l'ensemble de leur réseau et de leurs systèmes de protection des données. En évaluant l'efficacité des contrôles techniques et procéduraux en place, et en automatisant la vérification régulière des contrôles techniques (de paramètres de mot de passe, de configuration de serveur et de pare-feu, de gestion des correctifs, etc.), les entreprises peuvent réduire le risque de fuites de données. Pour maintenir et améliorer leur situation en matière de conformité, les entreprises doivent constamment évaluer la configuration de leur infrastructure informatique par rapport aux politiques de mise en conformité. La création et le déploiement de politiques, l'évaluation des contrôles de conformité informatique, la gestion des incidents et l'utilisation d'outils de corrélation vous permettent d'identifier et de réduire proactivement les insuffisances avant que des fuites ne se produisent et, en cas d'attaque, d'identifier et de hiérarchiser les risques d'un bout à l'autre de l'entreprise.

- Définir des politiques informatiques fondées sur les pratiques d'excellence en matière de sécurité des données et des normes industrielles telles qu'ISO 17799, COBIT, NIST SP800-53, Sarbanes-Oxley, PCI DSS, HIPAA, GLBA et bien d'autres.
- Aligner les politiques informatiques sur les principaux contrôles opérationnels et de sécurité, tant procéduraux que techniques.
- Automatiser l'évaluation de l'infrastructure et des systèmes en fonction des contrôles de conformité informatique existants.
- Evaluer les performances de l'entreprise face aux contrôles de conformité informatique et les consigner dans des rapports.
- Hiérarchiser les mesures de résolution des problèmes en fonction des résultats de ces évaluations et rapports, et mettre proactivement à jour l'infrastructure et les systèmes de sécurité afin de démontrer la conformité et d'assurer une sécurité maximale.

Etape 5. Prévenir l'exfiltration des données. En cas d'incursion d'un pirate, il est encore possible de prévenir une fuite de données au moyen d'un logiciel réseau permettant de détecter et de bloquer l'exfiltration des données confidentielles. Les fuites imputables à des employés peuvent également être identifiées et arrêtées. Les solutions de prévention des pertes et de gestion des événements liés à la sécurité peuvent opérer conjointement pour prévenir les fuites durant la phase de transmission des données sortantes.

- Surveiller et empêcher les fuites de données par le biais de transmissions réseau, qu'elles soient imputables à des programmes malveillants ou à des employés bien ou mal intentionnés.
- Identifier les transmissions vers des sites pirates connus et alerter les équipes de sécurité pour prévenir l'exfiltration de données confidentielles.

Etape 6. Intégrer les stratégies de prévention et de réponse aux opérations de sécurité. Pour prévenir les fuites de données, il est essentiel d'intégrer un plan de réponse et de prévention des fuites aux opérations quotidiennes de l'équipe de sécurité. En tirant parti de la technologie pour surveiller et protéger les informations, l'équipe de sécurité peut

Fuites de données, mode d'emploi

Pourquoi des fuites de données se produisent-elles et comment s'en prémunir ?

continuellement améliorer le plan établi et, ainsi, réduire progressivement les risques grâce à une connaissance toujours plus grande des menaces et des vulnérabilités.

- Intégrer les solutions de prévention des fuites de données, de protection des systèmes, de mise en conformité et de gestion de la sécurité afin de créer un modèle opérationnel de sécurité fondé sur les risques et sensible au contenu, immédiatement réactif aux menaces et piloté par workflow afin d'automatiser les processus quotidiens et de combler les espaces entre les individus, les politiques et les technologies.
- Mettre à profit les services de sécurité (notamment de conseil, de formation, de support intégral et d'informations globales) qui procurent aux entreprises une connaissance en profondeur de la sécurité et une expertise dans les produits de sécurité.

Pour une vue générale des solutions Symantec permettant de mettre un terme aux fuites de données, reportez-vous à l'annexe.

Comment démarrer ?

La première étape consiste à créer un plan de prévention et de réponse en vue d'identifier les types d'information à protéger et l'emplacement de ces informations dans votre entreprise. Une fois que vous avez identifié les informations prioritaires et déterminé votre niveau de risque de perte de données, l'étape suivante consiste à évaluer votre réseau et à localiser les éléments de votre infrastructure qui vous rendent vulnérable aux attaques externes.

Pour bon nombre d'entreprises, ce processus commence par une évaluation des risques sur site. Le service Information Exposure Assessment proposé par Symantec offre aux clients une vue globale et centrée sur les données du risque informatique dans l'entreprise. Avec ses services de conseil et ses technologies de référence en matière de prévention des pertes de données, Symantec est en position idéale pour fournir à ses clients une analyse détaillée de leur degré d'exposition aux vols de données internes et externes ainsi qu'une évaluation quantitative des risques de pertes de données sur les réseaux, les applications Web, les dispositifs de stockage et les terminaux. Cette approche combinée permet à Symantec de produire un plan de réduction des risques détaillé et complet spécialement conçu pour gérer les problèmes de pertes de données sensibles et d'exposition des informations. Le plan d'action détaillé qui en résulte inclut des conseils pour la gestion des risques internes et externes et recommande diverses actions permettant de réduire et d'éliminer les zones d'exposition dans toute l'entreprise.

Pourquoi choisir Symantec ?

Symantec n'ignore pas que l'un des plus grands défis auxquels sont confrontées les entreprises d'aujourd'hui consiste à trouver un équilibre entre la disponibilité des données, indispensable à des fins opérationnelles, et la nécessité de mettre ces informations à l'abri de tout accès non autorisé. En souscrivant au service Exposure Assessment de Symantec, les clients acquièrent une compréhension et une visibilité uniques des risques auxquels sont exposées leurs informations et peuvent commencer à gérer proactivement ces risques par une approche coordonnée.

Symantec est le leader mondial en matière de sécurité et, de loin, l'éditeur de logiciels de sécurité le plus présent sur le marché. Nous protégeons plus de systèmes, d'entreprises et de communautés que tout autre éditeur. Symantec fournit les

Fuites de données, mode d'emploi

Pourquoi des fuites de données se produisent-elles et comment s'en prémunir ?

produits et services les plus nombreux et les plus prisés sur le marché. Nous offrons également la meilleure expertise en matière de sécurité et le plus vaste réseau d'informations international. Pour les entreprises qui ont besoin de protéger des informations vitales, de répondre rapidement à toute menace, de démontrer leur conformité et de gérer efficacement la sécurité, Symantec est reconnu comme l'interlocuteur idéal.

Annexe

Matrice de solutions de protection des informations de Symantec. Vous trouverez ci-dessous les méthodes commentées dans la session *Comment prévenir une fuite de données* du présent document, avec des références aux solutions de prévention proposées par Symantec.

Solution Symantec	Avantages
Symantec™ Data Loss Prevention for Storage	Visibilité des emplacements de stockage de vos données confidentielles et lancement d'actions automatisées qui protègent les données par le biais de quarantaines, du chiffrement ou de technologies ERM (Enterprise Rights Management). Surveillance de l'activité du personnel sur le réseau et les terminaux, même quand les utilisateurs sont déconnectés du réseau d'entreprise. Arrêt des pertes de données confidentielles. Mise en quarantaine, copie et suppression automatiques des données stockées sans raison valable. Protection des terminaux, que l'utilisateur soit ou non connecté au réseau de l'entreprise. Application automatique des politiques DLP universelles grâce à une plate-forme centralisée pour la détection, les processus de résolution des incidents, la création de rapports, la gestion et la sécurisation du système.
Symantec™ Protection Suite	Sécurisation de votre environnement contre les programmes malveillants, le spam, les réseaux de bots et les menaces du Web 2.0 grâce à l'unification et à la précision des méthodes d'identification et de traitement des risques pour toutes les Sécurisation des données sensibles et des informations confidentielles au niveau de la passerelle avec le filtrage avancé de contenu et la prévention des pertes de données. Informations sur la sécurité fournies en temps réel, déclenchant des alertes anticipées en cas de danger et assurant une protection proactive contre les nouvelles menaces.
Symantec™ Control Compliance Suite	Définition et application dans toute l'entreprise d'une politique de protection des données confidentielles. Évaluation automatique de l'efficacité des contrôles techniques et procéduraux dans l'application des politiques de mise en Importation d'informations sur les ressources et contrôle des données issues de périphériques et d'applications tiers, tels que les solutions de prévention des pertes de données, afin d'évaluer l'efficacité des contrôles. Création pour chaque politique de rapports sur la conformité de type tableau de bord reposant sur les rôles. Prévention des défaillances par une hiérarchisation des risques.
Altiris™ Total Management Suite de Symantec	Alignement des processus sur les pratiques d'excellence du marché pour une gestion plus efficace des systèmes client et serveur. Gestion du cycle de vie complet incluant des fonctions intégrées de déploiement, de gestion des systèmes actifs et de surveillance accessibles depuis une console centralisée. Regroupement de la gestion des services et des ressources de l'entreprise dans une architecture, un référentiel et une Amélioration de la disponibilité et des niveaux de service, et réduction des coûts au moyen de puissants outils ITIL de gestion des incidents, des problèmes, des modifications et des connaissances.
Évaluation de l'exposition des informations : un service de Symantec	Acquisition d'une meilleure compréhension de la façon dont les données confidentielles sont utilisées et stockées dans l'entreprise. Réalisation d'une évaluation en profondeur des risques de perte de vos données. Lancement de tests ciblés de pénétration des réseaux, des systèmes et des applications contenant des informations Reporting sur les vulnérabilités qui peuvent être mises à profit par des pirates internes ou externes pour accéder aux informations stratégiques.

A propos de Symantec

Symantec est l'un des principaux fournisseurs mondiaux de solutions de gestion de la sécurité, du stockage et des systèmes permettant aux particuliers et aux entreprises de protéger et de gérer leurs informations. Les logiciels et services de Symantec assurent la sécurité de l'information là où elle est utilisée ou stockée grâce à une protection complète et efficace contre toutes sortes de risques.

Pour connaître les coordonnées des bureaux dans un pays spécifique, consultez notre site Web.

Symantec (France) S.A.S.
17 avenue de l'Arche
92671 Courbevoie Cedex
01 41 38 57 00
www.symantec.com/fr

Copyright © 2010 Symantec Corporation. Tous droits réservés. Symantec et le logo Symantec sont des marques commerciales ou des marques déposées de Symantec Corporation ou de ses filiales aux Etats-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs. LIMITATION DE GARANTIE. Les informations communiquées dans le présent document vous sont fournies "EN L'ETAT" et Symantec Corporation ne concède aucune garantie en ce qui concerne leur exactitude ou leur utilisation. Toute utilisation des informations contenues dans les présentes se fait aux risques de l'utilisateur. Le présent document peut contenir des inexactitudes techniques ou d'une autre nature ainsi que des erreurs typographiques. Symantec se réserve le droit de modifier ces informations sans préavis.
8/2010 20049424-1